Report on information obtained from

PW CS/2318 Obstlt METTIG OKW/WFsT/Ag WNV/Chi

captured at RHEIMS 15 May 1945

- - - - - - - - - -

# HISTORY AND ACHIEVEMENTS OF THE CRYPTOGRAPHIC SECTION OF THE OKH

## (OKH/AHA/In 7/VI)

## PREAMBLE

This report supplements information already published by CSDIC (UK) in SIR 1335 and 1704. Although the information in this report is of a general nature, it gives a fairly complete picture of the German aims and achievements in he cryptographic field, seen through PW's personal position as head of the OKH cryptographic section from Nov. 41 to June 43. In general, PW has been connected with the work of the "Y" service in an organisational capacity from 1935 onwards. His memory is reasonably good, though he is less well-informed on technical matters of cryptography. Although a slight tendency to hedge on vital questions was observed, it would appear that PW has not now withheld anything of importance.

His life history is as follows:

| | |
|---|---|
| 1933 | Took comd of Horchkp of Nachr Abt I. |
| 1935 - 39 | Comd Horchkp of Nachr Abt 25. |
| Sep 39 - Apr 40 | Comd 3 Coy Nachr Abt 750. (This coy was on intercept duties opposite the Maginot Line.) |
| Apr 40 - Summer 40 | Senior Sigs Intelligence Officer with Army Group C. |
| Summer 40 - Nov 41 | Comd Nachr Abt 26. |
| Nov. 41 - Jun 43 | Comd OKH/In 7/VI. |
| Jun 43 - Dec 43 | Comd Pz Korps Nachr Abt 448. |
| Dec 43 - Apr 45 | In charge of OKW/Chi Hauptgruppe A. |
| May 45 | In charge of OKW/Chi in the closing stages. Went on FLENSBURG mission to SHAEF, and thence into Allied captivity. |

## HISTORY OF IN 7/VI

ORIGINS

Before the war, cryptography in the German Army was carried out by OKH/In 7 Horchleitstelle. This organisation originated in the cipher section of the German War Ministry, and grew up parallel with the cipher section of the OKW (OKW/Chi). Before the war, In 7 Horchleitstelle was merely a small department. It was commanded by Major Dr. JUNG, and had a number of fixed intercept stations (FNAST) under it. These were staffed by a skeleton organisation, and were engaged in monitoring the menoeuvring traffic of neighbouring states.

PRE-WAR ACTIVITIES

General

The Horchleitstelle before the war was principally engaged in intercepting traffic in FRANCE, BELGIUM, HOLLAND, POLAND and RUSSIA; SWITZERLAND was only casually monitored. The main successes were gained at the expense of FRANCE, HOLLAND and RUSSIA.

RUSSIA

The Germans were able during the first Russo-Finnish war, to break a number of Russian 2-, 3- and 4-figure codes. In addition, a copy of the Russian 5-figure code was obtained; this was handed over by the Finnish General Staff. This particular code was used by the Russians in the first year of the war with GERMANY.

HOLLAND

An exercise of the Dutch Army was covered in 1937. Very simple techniques, principally double transposition ciphers, were used, and these could be read without much difficulty. As a result, it was possible to establish the order of battle of the Dutch units participating in the exercise down to Bn level.

FRANCE

Continuous and significant successes were obtained against the French before the war. Before 1939 the Germans covered the French static wireless net which radiated from PARIS to the static formations in FRANCE. Cipher procedures were continuously read, and provided valuable information during the international crises of 1937, spring and autumn 38, and 1939. PW cannot detail which exact ciphers were read.

BRITAIN

Very little success was obtained in the reading of British ciphers before the war; this PW attributes to the very poor quality of the personnel employed on the task.

STATIC PERIOD 1939-40

General

The Sigs Intelligence picture provided during the early period of the war was good. The complete picture of British, French and Dutch orders of battle was available. Changes in that order could always be followed. It should be noted, however, that whereas the French, Belgian and Dutch picture was partly obtained as a result of crypto-analytical achievements, the order of battle of the British Army could only be built up by the result of DF information, and the evaluation of call-signs and other items of WT procedure.

French

In 1939, the Germans cracked the "mobile" cipher which had replaced the peace-time cipher of the static French wireless net with the outbreak of war. All messages on this net could be read, and though they were of an administrative or supply nature, nevertheless helped to fill in the tactical picture. For example, the strength

of units being set up on the training ground at MOURMELON was estimated by statistics of water bottles and blankets. It was equally possible to deduce facts about the shortage of armour-piercing amn with the French inf units. Similarly, the conversion of the 2nd and 3rd French Cav Divs to Armoured Divs in the area north east of PARIS was ascertained in Dec 39. Likewise, the order of battle of the French 6th Army on the French-Italian border was speedily learnt.

Polish

Owing to the speedy development of the Polish campaign, very little cryptographic work was undertaken. The main sigs intelligence information on the regrouping of the Polish forces was derived from the Polish rly WT traffic which PY believes was carried out in clear.

GERMAN OFFENSIVE May-Jun 40

FRANCE

With the opening of the offensive in May 40, the French began to use ciphers in increasing quantities. The Germans soon felt an acute shortage of forward cryptographers and were therefore unable to undertake much work on the French forward ciphers. As a result, the forward units concentrated on the two French cipher machines, the B-211 and C-36. Progress was slow, but as a result of research on two captured C-36 machines, Army Group C was in a position, by Jul 40, to undertake satisfactory reading of the traffic. Likewise it was impossible to break the B-211 machines in time for that information to be of any value. Nevertheless the research undertaken during this period was to justify itself later.

GREAT BRITAIN

Although similar success was achieved against Dutch and Belgian ciphers, the Germans still failed to break into any important British procedures. The English cryptographers, consisting of six personnel from the Horchleitstelle, were put to work at BAD GODESBERG, but in spite of good supply of material, they failed to achieve any success.

SUPPLIES OF CRYPTOGRAPHERS IN THE WEST 1939/40

When the forward intercept units moved into the field in 1939, no cryptographers were available. Obst RENDEWIG, the Comd of all intercept units in the WEST, was able to procure a number of cryptographers from "Y" units around BERLIN and filled that number out by calling in a number of mathematicians and linguists. As a result, when the German offensive started in Apr 40, the "Y" units with the army groups contrived to have a moderate supply of crypto-analytic personnel.

REORGANISATION OF IN 7 HORCHLEITSTELLE

The experiences of 1940 showed that considerable expansion in the German Army cryptographic service was desirable. This reorganisation was carried out by Major MANG. His aim was not only to increase the crypto-analytic staff at the centre, but also to provide reserves of cryptographers to work in certain key areas. The cryptographic section thereupon became independent and was reorganised as Gruppe VI of In 7. Henceforth it was subordinated to the reserve army for personnel and administrative matters, but remained subordinated to Chef HNW of Field Army for matters of policy. It would have been more logical to have made the cryptographic section a department of Chef HNW, just as Horchleitstelle was converted to Gruppe IV. Nevertheless this curious form of organisation paid, and enabled the cryptographic service to recruit sufficient personnel without serious interference.

In general, the object of In 7/VI was the organisation and conduct of crypto-analysis in the field and in the rear; training of cryptographers and the investigation of the security of German ciphers.

It was also felt that in certain critical regions, an extra crypto-analytic effort should be enforced. To this end, the Russian Referat of In 7/VI was detached to the Horchleitstelle LÖTZEN, while special crypto-analytic sections for British traffic were detached to the Horchkp SELBOHM and the Kommandeur for Horchtruppen 4 in ATHENS (See SIR 1704, para 45, and Appendix 6.)

ORGANISATION

General

PW can add little to SIR 1335 and 1704. In 7/VI in 1942 consisted of the following Referate:

| | |
|---|---|
| Referat Z. | Hptm HERBRÜGGEN |
| English Referat: | Oberinspektor ZILLMANN, with forward sections in: NORTH AFRICA, under Kriegsverwaltungsinspektor HARMS<br>ATHENS, under Oblt KNESCHKE<br>PARIS, under major HENTZE<br>BERGEN, under oberinspektor PFITZER |
| French Referat: | Sonderführer KUHN, with subsections dealing with Swiss, Spanish, Portuguese and Brazilian traffic. |
| Balkan Referat: | Reg Rat BAILOVITCH |
| Russian Referat: | Kriegsverwaltungsinspektor DETTMANN (detached to LÖTZEN) |
| Italian Referat: | Hptm Dr FIALA |
| Agents Referat: | Oblt Dr VAUCK |
| Hollerith Referat: | Kriegsverwaltungsrat SCHENKE |

Training Referat: Oberinspektor KUHN

Linguistic Referat. Sonderführer KÖHLER

American Referat: Sonderführer (Z) STEINBERG

Mathematical Referat: Sonderführer Dr PIETSCH

Reorganisation of Referat PIETSCH

In 1942, the Mathematical Referat had expanded to such an extent that three sections were created out of it. Sonderführer STEINBERG and the mathematicians who had been working with him on M-209 and the strip cipher separated to form the American Referat while two separate sections were formed, one under Oblt LÜDERS for the investigation of cipher security, and one under Wm Dr DÖRING for the investigation of secret teleprinters.

WORK OF HOLLERITH REFERAT

The Hollerith Referat was commanded by Baurat SCHENKE. The department was equipped with all kinds of German machines and also with all kinds of captured French hollerith equipment. This dept proved invaluable in the investigations of unclear or difficult cipher techniques. A lot of time and manpower was saved, particularly in the sorting out of traffic and the ascertaining of parallelisms and in the calculation of recurring differences. The exploitation of hollerith methods was particularly favoured by Baurat SCHULZE, who in civilian life was an employee of the hollerith firm Berlin Lankwitz.

MATHEMATICAL REFERAT

Baurat Dr PIETSCH collected together in this section the best available mathematical brains. In this section all unbroken traffic from the National Sections was investigated so long as it was necessary to achieve an inroad by purely analytical methods. As soon as a technique for breaking a particular cipher was evolved the item was handed back for further work to the specific National Section concerned. In some cases mathematical specialists were attached to the National Section to work on the various national procedures.

A further large field of work of the Referat PIETSCH lay in the investigation of the security of the current German cipher procedures and in the assessment of discoveries that were always being brought forward. The compromising of the security of a cipher usually resulted from exceeding the day's safety margin for transmission, thus creating depth or by other breaches of standard operating instructions.

In order to provide some check on the use of German ciphers and to provide the Referat PIETSCH with the necessary material, the Nachr Aufkl Abt/ Chef H Rüst u BdE was set up in Berlin in Nov 41. This unit was to be under the comd of the Comd of In 7/VI. Two coys of this unit were to act as normal holding coys for In 7/VI while the third was an intercept coy which worked within the field and Reserve Army for collecting material tocheck up on the security of German ciphers. However, at the

end of Feb 42 this unit was dissolved owing to personnel shortage. Thus the control of cipher security became once more the responsibility of the Field Army, a responsibility which was never fully undertaken.

As a result of the security investigation of German ciphers and the reporting on new discoveries, the Referat PIETSCH naturally began to develop new cipher techniques of its own. In 1942, however, the development of these techniques was handed over to OKW/Chi. The main investigation carried out by Referat PIETSCH was a continual enquiry into the security of the German cipher machine, the enigma which higher authority had been worried about for some time. The cause of this anxiety lay in the fact that it had been established before the war that CZECHOSLOVAKIA in collaboration with FRANCE had been able to read traffic enciphered by the enigma machine (old model without plug and socket connections). Evidence on this subject was captured during the occupation of CZECHOSLOVAKIA during 1938. Moreover in POLAND in 1939 the clear version of a WT message was found; this message had been transmitted from a German cruiser in Spanish waters during the Spanish Civil War and had been transmitted by the enigma officers' cipher. An exact proof whether these successes were due to compromise or to crypto-analytic work was never forthcoming, despite detailed investigation. As this instance of compromise affected the Stecker Enigma investigations were carried out thoroughly. The Polish cipher HQ at WICHER was searched in 1939. In subsequent years even 1943 and 44 Gen FELLGIEBEL ordered the reinterrogation of Polish cryptographers to check this point. No positive confirmation was achieved.

Nevertheless these investigations showed that the safety margin of the enigma had to be reduced from 50,000 to 20,000 letters on a day's cipher (an experience which resulted in the daily cipher, which at the beginning of the Russian campaign was very heavily burdened, being split up into two or three portions). As the final result of the enigma investigations described above, the value of carrying out investigations into machine cipher of enemy nations was recognised and the process undertaken.

TRAINING REFERAT

Until 1942 the work of this section was not fully exploited and only a small beginners' course was in progress.

It is fitting at this juncture, therefore, to draw attention to the acute shortage in crypto-analytic personnel which the German High Command encountered. It was found that the practice of pushing forward groups of crypto-analysts to key areas did not of itself provide adequate signals intelligence, particularly as the front lines were getting further away from BERLIN.

As a result the comds of forward intercept units were allowed to create their own crypto-analytic teams. Two difficulties were encountered

in this connection: firstly, a lack of technical knowledge, and secondly the entry into the crypto-analytic service of personnel who were untrustworthy from the security point of view. In two cases in KNA 2 in SMOLENSK personnel were unearthed who were guilty of espionage. As a result of this a security vetting for all crypto-analytic personnel was introduced.

Once the forward crypto-analytic units had been set up and attached to the various forward "Y" units it was agreed to allot to them the investigation of forward and L of C traffic which could be solved in the field. In 7/VI remained, however, responsible for all army crypto-analytic work and concentrated on the most difficult and unsolved procedures.

As a personnel establishment for these forward crypto-analytic units it was found necessary to have two or three linguists and one to three mathematicians. Such personnel were trained at a six weeks' course by In 7/VI. 200 such crypto-analysts were turned out; they included Major Dr HENTZE, Oblt Dr VAUK, Oblt LÜDERS and Oblt SCHUBERT. The results of this work in 1941 and 1942 was to enable In 7/VI to concentrate on research into more difficult procedures.

RUSSIAN REFERAT

This dept has had a rather curious history in that it was detached to Chef HNW Horchleitstelle/ LÖTZEN before the outbreak of hostilities with RUSSIA. Under the leadership of Kriegsverwaltungsinspektor DETTMANN, and for a time of Prof NOVOPASCHENNY this section achieved considerable initial success until spring 1942. The 5-figure code acquired by the Germans until the Russian-Finnish war was still used by the Russians. An additional copy of this procedure was also captured by the Germans. Through the allocation of call-signs and of indicator groups it was possible to establish the entire Russian order of battle and the location of strategical reserves. This was additional to intelligence gained by reading the content of traffic. On 1 Apr 42 the Russians introduced a new 5-figure code. The transition from the old to the new code was, however, so faulty that within the first week it was possible to establish 2,000 groups of the new code. Indeed, it was possible at this time to leave the decoding of this procedure to the cryptographers of the forward "Y" units. The Russians gradually improved their security, however, and in spring 1943 altered the indicator group system and split up the code into various front sectors. As a result it was necessary to collect all the 5-figure traffic at LOTZEN and to call in the assistance of the hollerith dept of In 7/VI. Only thus could the necessary depth on a day's traffic be achieved. The quantity of traffic read decreased considerably. 2-, 3- and 4-figure traffic was continuously decoded.

Crypto-analytic work on partisan traffic was carried on by the forward "Y" units in the area. Particular success was achieved in the SMOLENSK area with the arrival of specialist cryptographers.

It was only in the summer of 1943, however, when KNA 6, with Oblt SCHUBERT in charge of the cryptographers, was committed to anti-partisan work that the traffic between MOSCOW and the partisans was successfully read.

BRITISH REFERAT

This dept under Oberinspektor ZILLMAN was assisted in its early days by the successes of its forward cryptographic teams. These successes, however, were restricted purely to forward techniques.

In spite of continual efforts, Oberinspektor ZILLMAN was unable to break into the British cipher machine (Typex). Several British cipher machines were captured during the summer campaign of 1940, but with all of them the wheels were missing.

The general success of British Referat ceased, therefore, in the summer of 1942 after the intercept coy under Oblt SEEBOHM was captured in NORTH AFRICA. Despite the report of an NCO to the crypto-analytic section who escaped that all cipher material had been destroyed, it had obviously proved possible for the British to recognise from other evidence which British procedures had been read and which had not. In consequence the department was reinforced in order to win back the lost ground. Up to Jun 43 the lost ground had not been recovered and successes after that date are not known to PW.

From summer 1942 the Germans concentrated on watching exercise traffic in the BRITISH ISLES from KNA 5 in ST. GERMAIN and the Horchstelle BERGEN. Horchstelle BERGEN also watched Swedish traffic, but apart from unimportant police wireless there was very little army traffic to give depth enough to break the Hagelin machine which was used. This work was directed by Oberinspektor PFITZER.

As a result of watching the exercise traffic in ENGLAND it was still not possible to gain any assistance in winning back the lost ground in Mediterranean traffic; (cf SIR 1704, paras 61 to 64). It was nevertheless possible to gain some information on the training and order of battle for the invasion, but to what extent this was achieved by crypto-analytic methods is a matter which PW cannot answer owing to his departure to the Russian front.

REFERAT FRANCE

This section lost a lot of its importance after the campaign of 1940. It concentrated on watching the communications of the VICHY Government which was supposed to inform the Germans of their cipher procedures. Breaches of regulations committed by the French were reported to the Disarmament Commission at WIESBADEN and rectified. The retention of captured French documents and the further investigation of the French cipher machines C-36 and B-211 justified itself in that the initial de Gaullist WT traffic in NORTH AFRICA for 1942-43 was undertaken through these methods. It was possible to read all these techniques at the start but how far the success was maintained during 1943 PW cannot say.

The monitoring of Spanish, Portuguese and Swiss traffic which was coordinated by the French Referat did not yield any startling developments. In addition in the winter of 1942-43 two Brazilian techniques were read by this section. One of these, although its content was uninteresting, revealed one important feature; this message was passed along the link BRAZIL - WASHINGTON and travelled by American cipher to an American border wireless station; thence it was transferred to Brazilian cipher. The Brazilian cipher was broken, but the content of the message was unimportant. Nevertheless the effort to utilise the success to crack American cipher failed.

AMERICAN REFERAT

This dept was created in the winter of 1941-42 out of the Mathematical Referat. At the start the work of this dept was exceedingly difficult owing to the vast size of the American wireless net and the difficulty of sorting out the numerous links and cipher procedures employed. After some weeks order was obtained in reading the call signs and indicator groups and a start made in breaking some of the ciphers. The dept monitored internal American traffic and also traffic from the UNITED STATES to EUROPE and AFRICA. The Germans knew that the AMERICAN Government had bought the Hagelin machine which had formerly been offered in vain to the GERMAN Government. An immediate investigation of this procedure was therefore entrusted to Referat PIETSCH. Attempts to procure a model of the machine, however, proved unsuccessful. The bulk of material that accumulated grew so big, however, that a special team in the American Referat was entrusted with the investigation of this machine. By careful establishment of addresses and signatures the first inroads into the machine were obtained. Additional assistance was obtained through signals intelligence on the order of battle of the American Army in EUROPE; this enabled specimen messages to be assumed. However, it was eventually recognised that the main cipher procedure used by the Americans was the strip method whereby 25 variously arranged alphabets were vertically laid out one alongside the other. In the workshop of In 7/VI mechanical aids were constructed and with the help of the hollerith section and by noting the addresses and signatures the various alphabets were recreated. From spring 1942 parts of the American traffic were read, particularly traffic from WASHINGTON to WEST AFRICA, NORTH AFRICA and IRELAND. Latterly traffic from WASHINGTON to BRITAIN and WASHINGTON to CAIRO was also read.

It was also suspected in the American Referat that there was a decimetre link from LONDON to WASHINGTON relayed via IRELAND. This link was watched in its projection on the WEST coast of NORWAY and near NARVA on the BALTIC. The experiment proved unsuccessful and the source of this theory is unknown to PW.

With the arrival of American troops in BRITAIN their exercise traffic was continuously read. PW notes in this respect what he has already observed with regard to the M-209, that it is not surprising that traffic is read when mistakes in the use of ciphers were made in every three messages.

BALKAN REFERAT

PW cannot add much to SIR 1704. Work on Turkish traffic was not very profitable; a certain amount of army traffic was intercepted along the coast to the AEGEAN SEA, but its content was unimportant. The watching of Turkish traffic continued, however, as owing to TURKEY'S uncertain political game it was undesirable to interrupt it. The watch crypto-analytically in the case of Hungarian, Rumanian and Bulgarian traffic was dropped owing to the prior manpower claims of the Russian front.

ITALIAN REFERAT

This section specialised in watching Italian traffic which was very insecure and most of which was read by the Germans, especially traffic from ITALY to NORTH AFRICA. In 1941 Hptm Dr FIALLA paid a visit to ROME, notified the Italians of their weakness and requested greater security. In spring 1942 Hptm BIGGI of the Italian Army paid a return visit to In 7/VI and was enlightened as to the German use of hollerith machines. The renewed request to the Italian for greater security in their cipher methods failed, just as the Italians were unable to set up their own hollerith section. In 7/VI had not, in any case, the authority to put any pressure on the Italians, moreover, the general opinion was that the Italian cipher department under Gen GAMBA was not competent enough to institute changes; (in matters of agents' ciphers the Italian section was more efficient). It was assumed by In 7/VI that German troop movements in AFRICA were betrayed to the British by the insecure Italian wireless.

WORK OF SECRET TELEPRINTER REFERAT

This section dealt with investigation of the security of German machines only, since there were no enemy machines available for testing. In the summer of 1942, the SIEMENS secret teleprinters T 52 a and b were in use, and T 52 c was in the course of distribution. These machines were developed by the Heereswaffenamt under the direction of Dr LIEBKNECHT of Wa Prüf 7. They were manufactured by the firms of SIEMENS and LORENZ, were checked for security by OKW/Chi and found satisfactory. Nevertheless, in the summer of 1942, when these machines were tested by Uffz Dr DÖRING of Inspektion 7/VI, it appeared that the cipher could be easily cracked. This was principally due to operators sending more than one communication over the same message cipher. This mistake frequently arose over long distance communications. In the autumn of 1942, it was also recognised that the T 52 c, despite the alteration in the individual message encipherment, could not be made secure. This was exceedingly awkward, as it was the latest available secret teleprinter and was also used in communications from GERMANY to neutral countries. Alterations were undertaken which led to the T 52 d. Owing to the fact that there was a shortage of spare parts and industry could not deliver the new machines sufficiently speedily, the High Command (largely out of wishful thinking) began to consider the misgivings of Inspektion 7/VI as unwarranted, since the enemy was not in a position to tap lines as was done in the security checks by the German personnel. This comforting thought was, however, dashed in 1942-43 when an entire cellar for tapping telephone and teleprinter traffic was raided in PARIS; this installation was technically excellently equipped. Early in 1943, Wm Dr DÖRING established by further investigations that

the T 52 d was not secure and that single messages could be solved. He did it in this way: each letter was characterised by five electrical impulses which could be indicated as either plus or minus (positive or negative). On the basis of these impulses DÖRING differentiated between letters having positive or negative qualities. An enciphered positive letter preserved its positive quality. Having established the plus/minus relationship of the text, it was possible to feed a suspected clear word through the message until it fitted correctly. Thence the message could be broken. As a result, a new alteration was made in the T 52 d from which the T 52 e emerged, which was regarded until the end of the war as secure.

Other existing cipher machines, the Schlüsselzusatz (SZ) 40/42, and the secret teleprinter (SFM T) '43, were more satisfactory and were regarded as secure. These were used in wireless teleprinter traffic.

WORK OF CIPHER SECURITY REFERAT

This section was commanded by Oblt LÜDERS and was established in autumn 1942. It was responsible not only for testing the security of ciphers but also for investigating numerous inventions which were passed back from troops in the field. These inventions did not prove very profitable. They showed the lamentable ignorance of the field army on cipher matters. As a result, specialists from Inspektion 7/VI visited the signals school at HALLE to give lectures on this subject. Otherwise this dept remained inactive, working parallel to its parent body under Dr PIETSCH.

LIAISON OF INSPEKTION 7/VI WITH OTHER CRYPTOGRAPHIC AGENCIES

The collaboration between the crypto-analytic depts of other services was slight because, in PW's words, the enemy used different cipher techniques in different arms of the services. With obscure enemy procedures different depts carried out research and exchanged information until it was possible for one service to recognise the cipher as its own when it would take over all responsibility. In Jun 42, Inspektion 7/VI undertook a considerable volume of Hollerith work for the Navy until that dept built up its own Hollerith section. Where fundamental difficulties were encountered it was usually customary to consult OKW/Chi, which was the leading authority.

USE OF MECHANICAL AIDS IN IN 7/VI

The collaboration between Inspektion 7/VI and OKW/Chi was relatively close. OKW/Chi never had a Hollerith section at its disposal but developed its own machine aids in a workshop. By the end of 1942, it appeared that the Hollerith section of In 7/VI did not meet all demands. It was, therefore, decided to enlarge the Referat SCHENKE (the Hollerith section) with the technical advice of the workshop dept of OKW/Chi, so that it would be in the position to construct special mechanical aids for crypto-analysis. It was planned to build these mechanical aids in sufficiently great quantities so that they could be used with the forward "Y" units.

The first machine planned was to have been tested in Aug 43. What became of it is not known to PW. The machine was designed to search for parallelisms and had a speed of 10,000 to the second(?). The machine was known as the Lichtabtastmachine.

RESEARCH PLANS

The need for using more machines in cryptoanalytic work revealed the development of cipher technique during the war. It was to be expected that the enemy would place the Germans before more and more difficult cipher problems as hostilities developed. It was considered desirable to set up a special research section under Dr PIETSCH in May 43. This section was to be responsible for research into all mathematical and analytical problems and was to be placed at the disposal of the various national sections. The dept was also to draw up a central cryptographic reference book based on the experiments of the several sections, which was to be available for the whole organisation. This plan was never brought to fruition.

DEVELOPMENT OF GERMAN CIPHER PROCEDURES

In Aug 42, Inspektion 7/VI was ordered to collaborate with In 7/IV in the setting up of a dept for the development of cipher procedures for the field army. It was considered undesirable that the personnel from Inspektion 7/IV and In 7/VI should work together in that they might be unduly influenced by one another. Inspektion 7/VI did not agree with this viewpoint and stated that the personnel responsible for developing ciphers must be in continuous contact with the latest achievements of cryptography in order that a foolproof procedure was evolved. This viewpoint was not recognised, and In 7/VI posted Sdf Dr FRICKE, Uffz KEHREN and Uffz JESSE to In 7/IV. This was necessary because the field army had no ciphers in reserve at all.

From Mar 42, Dr FRICKE developed the RASTER Schlüssel which was introduced into the army in 1944. It was interesting to note that the basis for the RASTER Schlüssel was a corresponding technique used in the British Army. The flaws in this procedure were rectified so as to make the German version foolproof.

# APPENDIX

## LIST OF CIPHER PROCEDURES

## BROKEN BY THE GERMANS

(This is a translation of a document in PW's possession. He cannot give any additional information to what has already been mentioned in the body of the report. The list is incomplete in PW's opinion)

1. USA

PMC
Army field code
Div field code
M 209
Strip system

2. GREAT BRITAIN

Syko, anna
Syllabic cipher
Codex
Phantom code
War Office cipher (latterly not solved)
Slidex
Transposition cipher
Double transposition cipher
Playfair

3. RUSSIA

2-, 3- and 4-figure techniques
Signal tables
5 figure traffic reciphered with "Blok nots"
NKVD - L of C traffic
Partisan ciphers. Double transposition and re-ciphered figure keys.

4. FRANCE

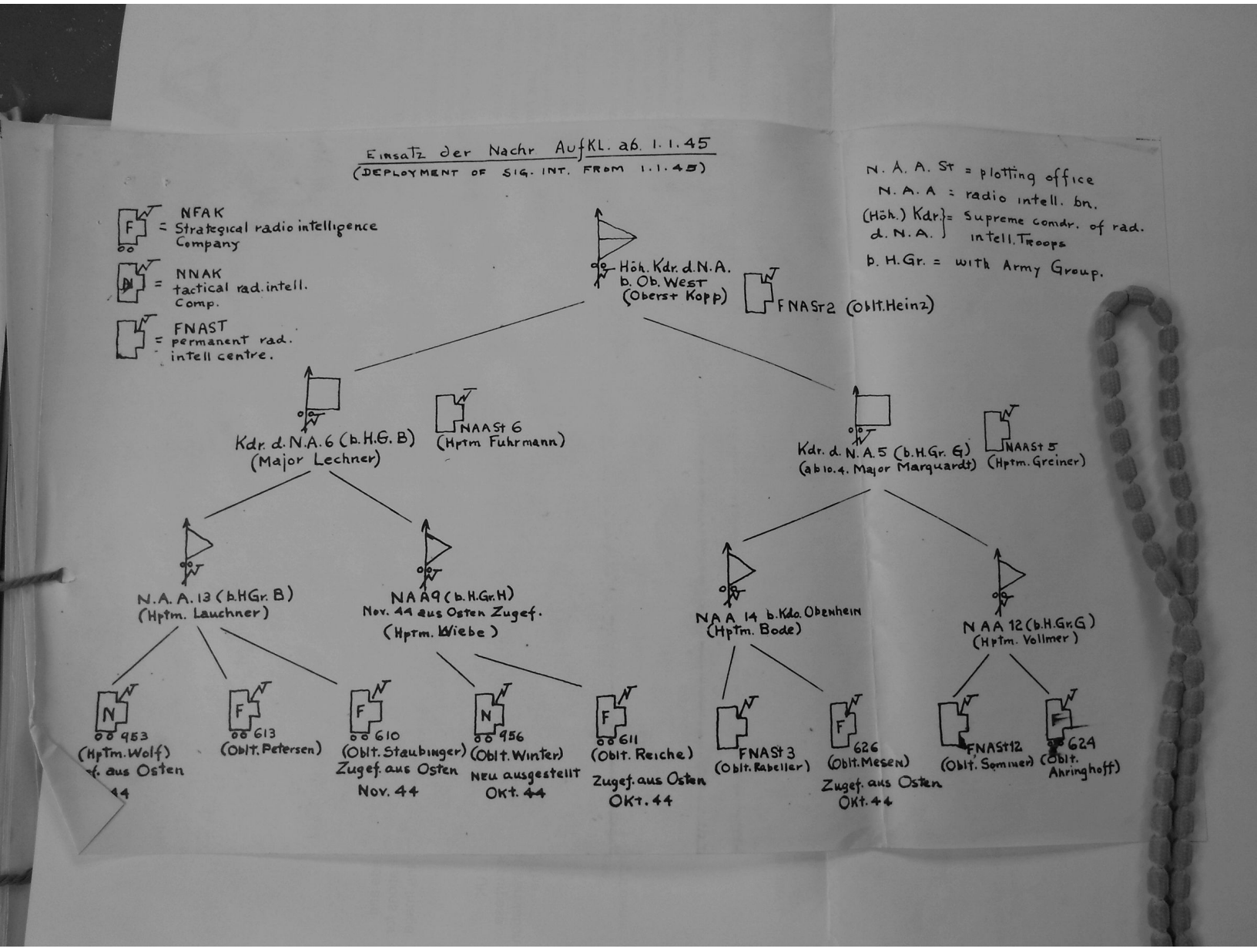
TSFF (reciphered code)
4-figure code - reciphered with square
Diagonally read single square
C-36 and B-211 machines

5. BELGIUM

Reciphered 3-figure code.

6. HOLLAND

Playfair


Einsatz der Nachr Aufkl. ab. 1.1.45
(DEPLOYMENT OF SIG. INT. FROM 1.1.45)
F = NFAK Strategical radio intelligence Company
N = NNAK tactical rad. intell. Comp.
= FNAST permanent rad. intell centre.
N. A. A. St = plotting office
N. A. A = radio intell. bn.
(Höh.) Kdr. d. N. A. = Supreme comdr. of rad. intell. Troops
b. H. Gr. = with Army Group.
Höh. Kdr. d. N. A. b. Ob. West (Oberst Kopp)
FNASt 2 (Oblt. Heinz)
Kdr. d. N. A. 6 (b. H. G. B) (Major Lechner)
NAASt 6 (Hptm Fuhrmann)
Kdr. d. N. A. 5 (b. H. Gr. G) (ab 10. 4. Major Marquardt)
NAASt 5 (Hptm. Greiner)
N. A. A. 13 (b. HGr. B) (Hptm. Lauchner)
NAA 9 (b. H. Gr. H) Nov. 44 aus Osten Zugef. (Hptm. Wiebe)
NAA 14 b. Kdo. Obenhein (Hptm. Bode)
NAA 12 (b. H. Gr. G) (Hptm. Vollmer)
N 953 (Hptm. Wolf) z. f. aus Osten 44
F 613 (Oblt. Petersen)
F 610 (Oblt. Staubinger) Zugef. aus Osten Nov. 44
N 956 (Oblt. Winter) Neu ausgestellt Okt. 44
F 611 (Oblt. Reiche) Zugef. aus Osten Okt. 44
FNASt 3 (Oblt. Rabeller)
F 626 (Oblt. Mesen) Zugef. aus Osten Okt. 44
FNASt 12 (Oblt. Sommer)
F 624 (Oblt. Ahringhoff)

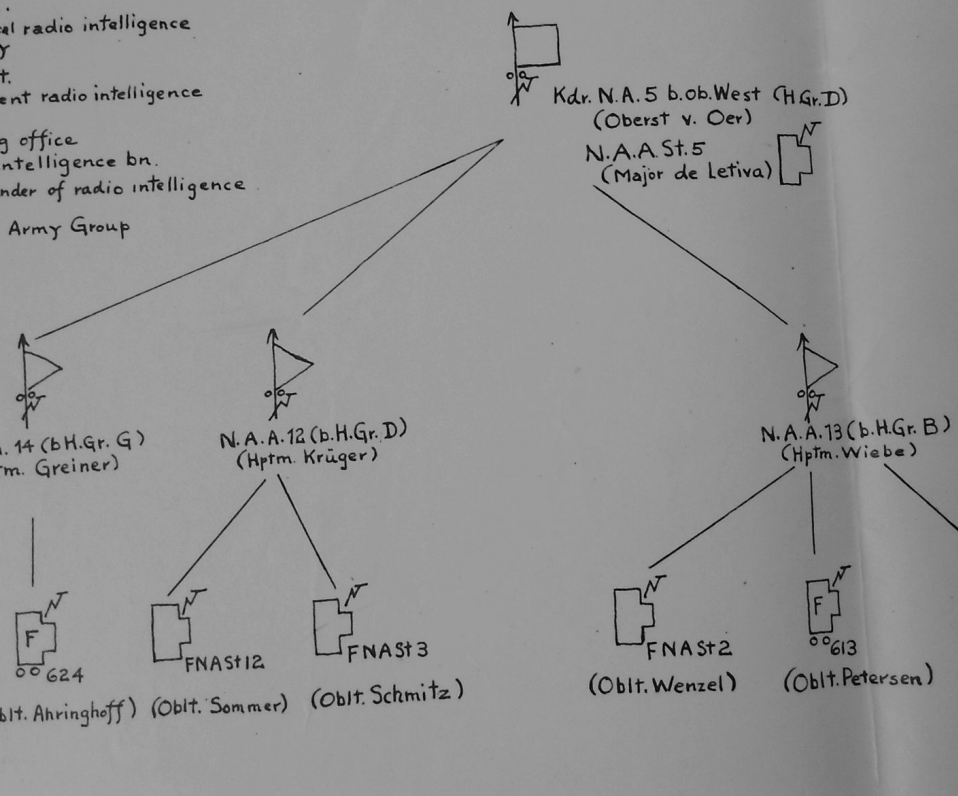
# Einsatz der Nachr. Aufkl. bei Beginn der Invasion
(DEPLOYMENT OF SIGNAL INTELLIGENCE AT BEGINNING OF INVASION)

Zeichenerklärung =

F = N.F.A.K. = Strategical radio intelligence Company

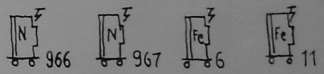
F.N.A.St. = permanent radio intelligence centre

NAASt. = plotting office
N.A.A. = radio intelligence bn.
Kdr. N.A. = commander of radio intelligence troops
b. H.Gr. = with Army Group

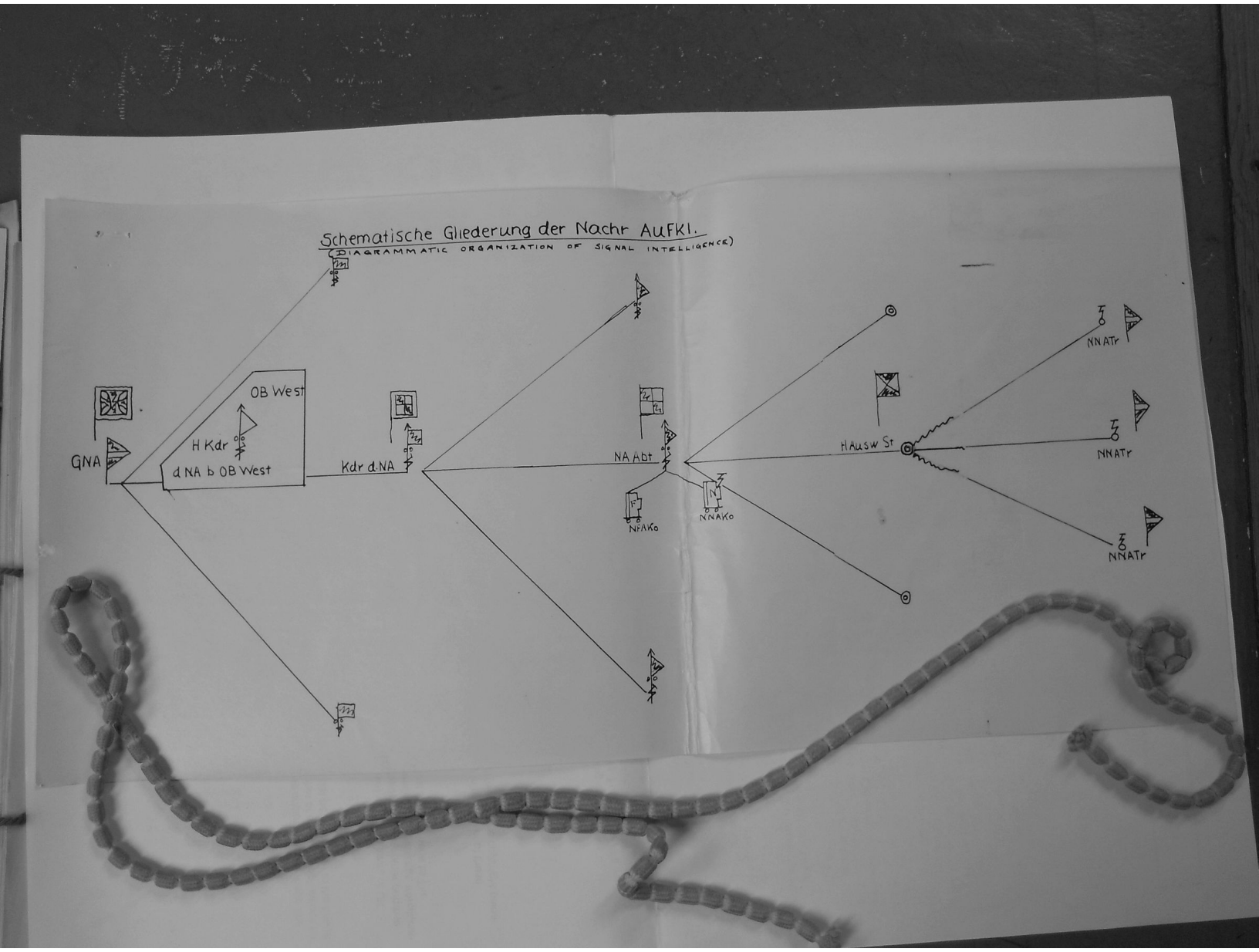


## Gliederung der Nachr. Aufkl.

(ORGANIZATION OF SIG. INTELLIGENCE)


| H.Gr. Mitte | H. Gr Weichsel | H.Gr. Kurland | OB West | H.Gr. G | H. Gr. H+B | H Gr C | H Gr Süd | Geb.AOK 20 | H. Gr. E |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | H Kdr b. OB West | 5 | 6 | 7 | 8 | 11 | 16 |
| NA Abt 3<br>" 4<br>" 5 | NA Abt 6<br>" 7<br>" 8 | NA Abt 10 | | NA Abt 12<br>" 14 | NA Abt 9<br>" 13 | NA Abt 17 | NA Abt 1<br>" 2 | | |


Schematische Gliederung der Nachr AufkI.
(DIAGRAMMATIC ORGANIZATION OF SIGNAL INTELLIGENCE)
OB West
H Kdr
d NA b OB West
GNA
Kdr d.NA
NA Abt
NNAKo
NNAKo
Hausw Sr
NNATr
NNATr
NNATr